PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-200730

(43)Date of publication of application : 31.07.1997

(51)Int.Cl. H04N 7/167
G09C 1/00
H04L 9/32
H04N 5/91
// H03M 7/30

(21)Application number : 08-003603

(22)Date of filing : 12.01.1996

(71)Applicant : CANON INC

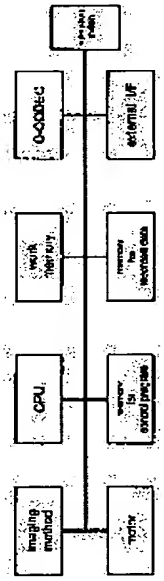
(72)Inventor : OISHI KAZUOMI

(54) DEVICE AND SYSTEM FOR VIDEO INPUT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a video input device with which the propriety of formed digital video data can be certified.

SOLUTION: This video input device for inputting an image and converting it digital is provided with a digital signature generating part C-CODEC for generating a digital signature for identifying these digital converted video data based on secrecy information (such as a cryptographic key to be used for the digital signature system of a public key encipher system, for example), specific to this video input device and these video data. Then, concerning the formed video data, the digital signature to be generated only by the video input device is found and the video data and the digital signature corresponding to these video data are defined as the output data of the video input device. Thus, any other device excepting for the video input device for forming certain video data can not generate the digital signature corresponding to these video data and when the output data are revised or forged, it can be detected.



LEGAL STATUS

[Date of request for examination] 11.12.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3260270

[Date of registration] 14.12.2001

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right] 12.03.2003

CLAIMS

[Claim(s)]
[Claim 1] The image input unit characterized by to have a means generate the information which performs a predetermined operation based on one [at least] information on the confidential information of a proper, and the digital data by which conversion was carried out [above-mentioned] to the external device connected to the above-mentioned image input unit at the confidential information and the above-mentioned image input unit of a proper, and identifies the above-mentioned digital data in the image input unit which inputs an image and is changed into digital data.
[Claim 2] The image input unit according to claim 1 characterized by performing the operation of the digital signature method using a public-key-encryption system as the above-mentioned predetermined operation.
[Claim 3] The image input unit according to claim 1 or 2 characterized by performing the above-mentioned predetermined operation at least in one side inside [where it connects with the interior of the above-mentioned image input unit, and the above-mentioned image input unit] an external device.
[Claim 4] An image input device given in any 1 term of claims 1-3 characterized by having a means to perform compression conversion to the digital data inputted and changed into the above-mentioned image input device, and a means to control to perform the above-mentioned predetermined operation to the data of the result by which compression conversion was carried out [above-mentioned].
[Claim 5] In the image input system which inputs an image and is changed into digital data To the external device connected to the above-mentioned image input system at the confidential information and the above-mentioned image input system of a proper, one [at least] information on the confidential information of a proper, A means to generate the information which performs a predetermined operation and identifies the above-mentioned digital data based on the digital data by which conversion was carried out [above-mentioned], Image input system characterized by having a means to verify whether it is that by which surely the digital data by which generation was carried out [above-mentioned] was generated by the above-mentioned image input system, using the information which identifies the above-mentioned digital data.
[Claim 6] Image input system according to claim 5 characterized by performing the operation of the digital signature method using a public-key-encryption system as the above-mentioned predetermined operation.
[Claim 7] Image input system according to claim 5 or 6 characterized by performing the above-mentioned predetermined operation at least in one side inside [where it connects with the interior of the above-mentioned image input system, and the above-mentioned image input system] an external device.
[Claim 8] Image input system given in any 1 term of claims 5-7 characterized by having a means to perform compression conversion to the digital data inputted and changed into the above-mentioned image input system, and a means to control to perform the above-mentioned predetermined operation to the data of the result by which compression conversion was carried out [above-mentioned].

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to an image input unit and image input system.
[0002]
[Description of the Prior Art] As for the image input device which inputs an image and forms digital image data, or image input system, it is common that highly-minute-izing of image data and high-definition-izing, and low cost-ization of equipment or a system are pursued. Therefore, research and development in the technique for coding with the sufficient input device of high resolution and effectiveness and a miniaturization etc. is done extensively.
[0003] On the other hand, incorporating the technique of guaranteeing surely the formed digital image data having been formed by the image input unit or image input system, as a function was seldom considered conventionally.
[0004]
[Problem(s) to be Solved by the Invention] Since the image formed in the image input device of an analog is analog data, in order to perform an alteration or forgery of the image data, special knowledge, capacity, etc. were required and it was rare for an alteration and forgery to be successful as a result. On the other hand, in the case of digital image data, since alteration and forgery may have been performed comparatively easily, there was a problem that the credibility of image data was low.
[0005] For example, since the image memorized by the negative film of a film photo is constituted by the silver salt molecule, it is difficult the image to detect this and to perform alteration and forgery. On the other hand, since the image currently expressed with the digital data consists of bit strings of 0 and 1, an alteration and forgery are easy to be performed using a computer. Therefore, the certification capacity as a factual proof can say digital image data that credibility is low small, and they have a possibility that an application may be limited.
[0006] It aims at offering the image input unit and image input system which accomplish this invention in order to solve such a problem, and enabled it to attest the justification of the formed digital image data.
[0007]
[Means for Solving the Problem] The image input device and system of this invention apply the digital signature which is a technique for guaranteeing the justification of digital data. According to a guide to code theoretical of Eiji Okamoto work (KYORITSU SHUPPAN Co., Ltd.), a digital signature "shows that surely the implementer of a message or information created them." That is, when digital data with a user and the subject (it is called an entity) who performs a communication link or computation of a calculating machine etc. is accepted, it is the digital data used as a proof which shows the fact.
[0008] The image input device of this invention asks for the digital signature which can generate only an image input device from the formed digital image data, and uses the image data itself and the digital signature corresponding to it as the output data of an image input device. And in the image input system of this invention, the entity which received the above-mentioned output data checks whether the correspondence relation between image data and a digital signature is realized correctly, and the data with which the relation corresponding to the right is not accepted presuppose that it is not just.

[0009] When anythings other than the image input device which forms a certain digital image data can generate the digital signature corresponding to the image data with an above-mentioned means and an alteration and forgery are made to output data, it becomes possible to detect it. Therefore, it becomes possible to guarantee that surely the image data was generated by the image input device, and the certification capacity as a factual proof can be given to digital image data.

[0010]

[Embodiment of the Invention]

[1st operation gestalt] This operation gestalt explains the case where it has public key encryption as confidential information of a proper inside an image input unit, using public key encryption as an algorithm of a digital signature. However, this is one example and what has a means to generate the information which identifies former information based on former information and confidential information instead of the digital signature algorithm using public key encryption is altogether contained in this operation gestalt.

[0011] Below, public key encryption is explained first. Next, about the configuration of an image input device, it explains and a concrete procedure in case the image input device of this operation gestalt which applied the digital signature using public key encryption generates a digital signature is described. Finally, a concrete procedure when verifying the digital signature is explained as a part of function of image input system.

[0012] While a cryptographic key and a decode key exhibit a cryptographic key unlike public-key-encryption public key encryption, it is the cipher system which holds a decode key secretly. Public key encryption can realize an authentication function for an addressee to check that the transmitting person of the sent correspondence not being a charlatan and its correspondence are not altered, and is considered to be the leading technique of realizing a digital signature.

[0013] For example, it is the open cryptographic key kp to Correspondence M. Encryption actuation performed by using is set to E (kp, M), and it is the secret decode key kS. If decode actuation performed by using is set to D (kS, M), a public-key-encryption algorithm will fulfill the following two conditions first.

(1) Cryptographic key kp When given, count of the encryption actuation E (kp, M) is easy. Moreover, decode key kS When given, count of the decode actuation D (kS, M) is easy.

(2) A user is the decode key kS. If it does not know, it will be a cryptographic key kp. Even if it knows the computational procedure and C=E (kp, M) of the encryption actuation E (kp, M), it is difficult to determine Correspondence M in respect of computational complexity.

[0014] Next, in addition to the conditions of the above (1) and (2), when the following conditions of (3) are satisfied, a secret communication function is realizable.

(3) The encryption actuation E (kp, M) can be defined to all the correspondence (plaintext) M, and D(kS, E (kp, M)) =M is materialized. That is, cryptographic key kp It is the decode key kS that D (kS, E (kp, M)) can be calculated and Correspondence M can be obtained although everyone can calculate encryption actuation E (kp, M) since it is opened to the public. He is only him who has.

[0015] On the other hand, in addition to the conditions of the above (1) and (2), an authentication function is realizable when the following conditions of (4) are satisfied.

(4) The decode actuation D (kS, M) can be defined to all the correspondence (plaintext) M, and E(kp, D (kS, M)) =M is materialized.

[0016] That is, it is the decode key kS that count of the decode actuation D (kS, M) can be performed. He is only him who has. Even if other men turn into him who calculates D (kS ', M) using fake private key kS ', and has the decode key kS and clear up, it is E (since it is kp and D(kS ', M) !=M, an addressee can recognize that the received information is unjust.). Moreover, even if the value of D (kS, M) is altered, it is set to E(kp, D(kS, M) ') !=M, and an addressee can check that the received information is unjust. This decode actuation D (kS, M) is called the digital signature to Correspondence M.

[0017] A typical public key cryptosystem is held to below. As a method which can ** performing above-mentioned secret communication and an authentication communication link RSA cryptograph (R.)

[L.Rivest,] [A.Shamir] and L.Adleman: "A method of obtaining digital sinnatures and public key cryptosystems" and Comm.of ACM 1987, R code (M. Rabin: "Digitalized signatures and public-key cryptosystems", MIT/LCS/TR -212, and Technical Report MIT.1979), W code (H. C.Williams: "A modificationof the RSA public-key encryption procedure" 6 IEEE Trans.Inf.Theory, IT-26, and 1980), MI code () [Matsumoto and Imai: "the new algorithm of a public-key-encryption system", Shingaku Giho, IT 82-84,] [1982;T.Matsumoto and H.Imai:"A class of asymmetriccryptosystems] There are based on polynomials overfinite rings", IEEE International Symp.on Infomation Theory, 1983, etc.

[0018] moreover, as a method only whose secret communication is possible MH code (R.) [C.Merkle and] M. E.Hellman: "Hidding infomation and signatures in trapdoor knapsacks", IEEETrans.Inf.Theory, IT-24, and 5 and 1987, GS signal (A.) [Shamir and R.E.Zippel: "On the security of the Merkle-Hellman cryptographic schme",] [IEEE Trans.Inf.] Theory, IT-26, and 3 and 1980, CR code (B.) [Chorand R.L.Rivest:"A] knapsack type public key cryptosystems based on arithmetric in finit field" and Proc.Crypto84, M code (R.) [J.McEliece:"A] public-key cryptosystem based on algebraic cording theory"DSN Progress Rwp., Jet Propulsion Lab., 1978, E code (T. E.ElGamal: "A Public key cryptosystem and a signature scheme based on discretre logarithm", Proc.Crypto 84, and 1984), There is a T code (12 on the other hand Shigeo Tsujii, formula", Shingaku Giho, IT85- using "matrix decomposition 1985) etc. [Public key encryption]

[0019] furthermore, as a method which can perform only an authentication communication link S code (A.) [Shamir:"A fast] signature scheme", Report MIT/LCS/TM -107, MIT laboratory for computer science, Cambridge, Mass., and 1978, L code () [KLieberherr:"Uniform] complexity and digital signature", Lecture Notes in Computer Science 115 Automata, Language and programming, Eighth ColloquiumAcre, Israel, and 1981, A GMY code (S. Goldwasser, S.Micali and A.Yao: "Strong signature schemes", ACM Symp.on Theory of Computing, 1983), GMR code (S. S.Micaliand R.L.Rivest: [Goldwasser and] "A "paradoxical" solution to the signature problem") [ACM Symp.] on Foundation of Computer Science and 1984, OSS code (H.) [Ong,] [C.P.Schnorr] and A.Shamir.: "An efficient signature scheme based on quadratic equation", ACMSymo.on Theory of Computing 1984, and OS code (Okamoto --) Shiroi, the digital signature method by :" polynomial operation, IEICE TRANSACTIONS (D), J68-D, 5, and 1985;T.Okamoto There are and A.Shiraisi: "A fast signature scheme based on quadratic inequaliteis", IEEE Symp.on Theory of Computing, 1984, etc.

[0020] The image input device of this operation gestalt which applied the digital signature using the configuration, next the above public key encryption of an image input device is explained using drawing 1 . Each square block shown in drawing 1 is the component of a functional order, and the line which connects them expresses a control bus and a data bus. imaging method is the image pick-up section, it photos the target photographic subject, changes it into an electrical signal, performs suitable signal processing, A/D-conversion processing, an image processing, information source coding processing, etc., and outputs digital data.

[0021] CPU is a central processing unit and performs predetermined count and control according to the control software memorized by memory for control program. Above-mentioned memory for control program is the memory section, and memorizes the above-mentioned control software fair. work memory It is the memory section and is used for a working-level month for CPU to calculate. operation switch is a control unit and is for the user who uses equipment to input various directions.

[0022] motor It is a device right hand side and the mechanical device of operation which is not illustrated according to control of CPU is controlled. memory for recorded data is the memory section, and records the image data which this equipment outputs, or its part. external I/F is the interface section with external devices, such as a computer or removable memory, and communicates image data, the control software, etc. between the above-mentioned external devices. C-CODEC It is the digital signature generation section and the digital signature to the inputted digital data is generated.

[0023] In such a configuration, the basic actuation in an image input is as follows. That is, when photoing a certain object and performing an image input, an operator inputs the directions from a control unit

operation switch. CPU follows the photography directions and the control software memorized by memory section memory for control program, and is the image pick-up section imaging method and the device right hand side motor. It is digital signature generation section C-CODEC about the digital data of the image which controlled, photoed the object and was formed of the photography. It inputs. Digital signature generation section C-CODEC The digital signature corresponding to the inputted digital data is generated.

[0024] And the digital signature corresponding to the image data and it which were formed by doing in this way is recorded on memory section memory for recorded data according to the directions from an operator, or is sent to an external device through interface external I/F with an external device, or the both are performed. In addition, once the digital data photoed and formed was recorded on memory section memory for recorded data, it is digital signature generation section C-CODEC. It may be inputted.

[0025] Next, the digital signature using public key encryption is applied to the above image input devices, and the case where it has a private key as confidential information of a proper in equipment is explained.

[0026] It is [private key / (decode key) / of the image input device by this operation gestalt / algorithm / skcam and / digital signature generation] Ecam about pkcam and a digital signature verification algorithm in Dcam and a public key (cryptographic key). It carries out. Private key skcam Digital signature generation algorithm Dcam Digital signature generation section C-CODEC It memorizes inside. Moreover, public key pkcam Digital signature verification algorithm Ecam It is known by the entity (it is called a verification person) which checks the justification of data at least.

[0027] In the above image input devices, a concrete procedure in case a digital signature is generated is as follows.

[0028] The digital image data I formed with the image input device of a digital signature generation book operation gestalt are digital signature generation section C-CODEC. It is inputted. Digital signature generation section C-CODEC Private key skcam memorized to the interior Digital signature generation algorithm Dcam Dcam (skcam, I) is calculated by using and it outputs as a digital signature. And the image data I and digital signature Dcam (skcam, I) which are obtained by doing in this way are recorded on memory section memory for recorded data, it is sent to an external device through interface external I/F with an external device, or the both are performed.

[0029] Moreover, a concrete procedure which verifies whether image data and the digital signature corresponding to it are the images which surely were inputted by the above-mentioned image input unit is as follows. In addition, the whole system also including the procedure of the verification which is described below in addition to an image input unit is called image input system.

[0030] The verification person who thought digital signature D'cam (skcam, I) to be digital signature verification image data I' is a public key pkcam. Digital signature verification algorithm Ecam It uses and is I'=Ecam (pkcam and D'cam (skcam, I)).

It checks whether it is **********.

[0031] Here, when an upper type is materialized, received image data I' is the image data I photoed with the above-mentioned image input device. On the other hand, when an upper type is not materialized, received image data I' is the image which is not the image data I photoed with the above-mentioned image input device. That is, it can be judged that it is not image data which the value of D'cam (skcam, I) is the case of ********, was photoed [from which the value of Dcam (skcam, I) differs, or both image data I' and digital signature D'cam (skcam, I) differ] with the above-mentioned equipment, and were formed.

[0032] [2nd operation gestalt] This operation gestalt explains the case where it has the private key of public key encryption as confidential information of a proper in the external device connected to an image input unit, using public key encryption as a digital signature algorithm, using drawing 1 .

[0033] It is Dman about skman and a digital signature generation algorithm in the private key stored in the pocket equipment (not shown) as an external device described below in this operation gestalt. It is

Eman about pkman and a digital signature verification algorithm in the public key which corresponds by carrying out. It carries out. Moreover, the above-mentioned pocket equipment is an information processor of a pocket mold, and is connected to an image input unit through interface external I/F with an external device in the case of photography. The entity (it is called a verification person) which checks the justification of image data is the digital signature verification algorithm Eman. Public key pkman It knows.

[0034] The basic actuation in an image input is as follows. That is, when photoing a certain object and performing an image input, the above-mentioned pocket equipment is connected to interface external I/F with the external device in an image input unit, and a photography person is a control unit operation. Directions of photography are inputted from switch. CPU follows the control software remembered to be the photography directions by memory section memory for control program, and is the image pick-up section imaging method and the device right hand side motor. It is the digital data of the image which controls, photos an object and is acquired by that cause Digital signature generation section C-CODEC It inputs.

[0035] CPU and pocket equipment communicate through interface external I/F with an external device. Thereby, it is digital signature generation section C-CODEC. Private key skman memorized by pocket equipment Digital signature generation algorithm Dman It obtains and asks for the digital signature to the image data formed by above-mentioned carrying out photography using such information.

[0036] Thus, the digital signature corresponding to the image data and it which were formed is recorded on memory section memory for recorded data according to the directions from an operator, or is sent to an external device through interface external I/F with an external device, or the both are performed. In addition, once the digital data photoed and formed was recorded on memory section memory for recorded data, it is digital signature generation section C-CODEC. It may be inputted.

[0037] In the above image input devices, a concrete procedure in case a digital signature is generated is as follows.

[0038] The digital signature generation CPU minds interface external I/F with an external device, and is a private key skman from pocket equipment. Digital signature generation algorithm Dman The memory section work memory in an image input unit It downloads to CPU. Next, Dman (skman, I) is calculated using the digital image data I formed within the image input device, and it is outputted as a digital signature. And the image data I and digital signature Dmam (skmam, I) which are obtained by doing in this way are recorded on memory section memory for recorded data, it is sent to an external device through interface external I/F with an external device, or the both are performed.

[0039] Moreover, a concrete procedure which verifies whether it is the image as which image data and the digital signature corresponding to it were inputted when surely above pocket equipment was connected is as follows.

[0040] The verification person who received digital signature verification record data (it considers as image data I' and digital signature D'man (skman, I)) is the digital signature verification algorithm Eman. Public key pkman It uses and is I'=Eman (pkman and D'man (skman, I)).
It checks whether it is **********.

[0041] Here, when an upper type is materialized, image I' of record data is the image I photoed when the above-mentioned pocket equipment was connected. On the other hand, when an upper type is not materialized, image I' of record data is the image which is not the image I photoed when the above-mentioned pocket equipment was connected. That is, it can be judged that the value of D'man (skman, I) is not image data with which the value of Dman (skman, I) was photoed when it was the case of ******** from which it differs or both image data I' and digital signature D'man (skman, I) differ and the above-mentioned pocket equipment was connected.

[0042] Therefore, in such image input system, if pocket equipment supports accuracy with the photography person at one to one, the system which guarantees that it is the image which the photography person photoed is realizable.

[0043] [3rd operation gestalt] With this operation gestalt, while having the private key of public key encryption as confidential information of a proper in the external device connected to an image input unit, using public key encryption as a digital signature algorithm, the pocket equipment has arithmetic proficiency and the case where the necessary procedure is taken for digital signature generation as follows is explained using drawing 1 .

[0044] The digital signature generation CPU sends the digital image data I formed within the image input device to pocket equipment through interface external I/F with an external device. Pocket equipment is the private key skman memorized to the interior. Digital signature Dman (skman, I) is calculated from the sent image data I using the digital signature generation algorithm Dman, and it is sent to an image input unit through interface external I/F with an external device.

[0045] And the image data I and digital signature Dman (skman, I) which were obtained by doing in this way are recorded on memory section memory for recorded data, it is sent to an external device through interface external I/F with an external device, or the both are performed.

[0046] Since it is the same as the operation gestalt of the digital signature verification 2nd, explanation is omitted.

[0047] [4th operation gestalt] This operation gestalt explains the case where both an image input unit and the pocket equipment which is the external device have the private key of public key encryption as confidential information of a proper, respectively, using drawing 1 , using public key encryption as a digital signature algorithm. In addition, processing of this operation gestalt is the same as the 1st operation gestalt and the 2nd operation gestalt except for the following digital signature generation and processing of verification.

[0048] The digital signature generation CPU minds interface external I/F with an external device, and is a private key skman from pocket equipment. Digital signature generation algorithm Dman The memory section work memory in an image input unit It downloads to CPU. Next, Dman (skman, I) is calculated from the digital image data I formed within the above-mentioned image input device, and it is the count result Digital signature generation section C-CODEC It inputs.

[0049] Digital signature generation section C-CODEC To the inputted data Dman (skman, I), count of Dcam (skcam and Dman (skman, I)) is performed, and the count result is outputted as a digital signature. Thus, the image data I and digital signature Dcam (skcam and Dman (skman, I)) which were formed are recorded on memory section memory for recorded data, or are sent to an external device through interface external I/F with an external device, or the both are performed.

[0050] Moreover, a concrete procedure whose image data and digital signature corresponding to it verify whether it is the image inputted with the above-mentioned image input unit when surely the above-mentioned pocket equipment is connected is as follows.

[0051] The verification person who received digital signature verification record data (it considers as image data I' and digital signature D'cam (skcam and Dman (skman, I))) It is the digital signature verification algorithm Ecam of a proper to an image input device. A public key pkcam And it is the digital signature verification algorithm Eman of a proper to pocket equipment. Public key pkman It uses and is I'=Eman (pkman and Ecam (pkcam and D'cam (skcam, Dman (skman, I)))).

It checks whether it is **********.

[0052] Here, when an upper type is materialized, image I' of record data is the image photoed when the above-mentioned pocket equipment was connected with the above-mentioned image input unit, but when an upper type is not materialized, it can be judged that it is a different image.

[0053] In addition, with the above-mentioned operation gestalt, although the sequence of digital signature generation was the order of an image input unit next with pocket equipment first, it is also possible to make it reverse and the sequence of verification also becomes reverse in that case. Moreover, it is also possible to generate and verify without relation the data with which both an image input device and pocket equipment signed in the sequence. Furthermore, digital signature generation algorithm Dman of pocket equipment It memorizes inside the image input unit and is a private key skman.

・It is also memorizable to pocket equipment.
[0054] [5th operation gestalt] Next, the case where a digital signature is generated to the data which compressed it instead of the image data to record using compression technology is explained. Here, suppose that compression conversion is expressed with c. The entity (it is called a verification person) which checks the justification of image data knows this compression conversion c. others -- above-mentioned the 1- it is the same as that of the 4th operation gestalt.
[0055] The digital signature generation CPU performs count of c (I) to the digital image data I formed in the image pick-up section imaging method in an image input device, and uses compressed data c (I) obtained by that cause instead of the image data I. other processings -- above-mentioned the 1- it is the same as that of the 4th operation gestalt. For example, if it is based in the case of the 1st operation gestalt and explains, the image data I and digital signature Dcam (skcam, c (I)) will be recorded on memory section memory for recorded data, it will be sent to an external device through interface external I/F with an external device, or the both will be performed.
[0056] Digital signature verification record data (the verification person who received image data I' and digital signature D'cam (referred to as skcam and c (I)) uses the digital signature verification algorithm Ecam and a public key pkcam, and is c(I') =Ecam (pkcam and D'cam (skcam, c (I))))
It checks whether it is **********. In addition, if the verification person knows the inverse transformation c-1 of compression conversion, it is I'=c-1 (Ecam (pkcam and D'cam (skcam, c (I)))).
** may be checked for whether it is **********.
[0057] Here, when an upper type is materialized, image I' of record data is the image photoed with the above-mentioned image input unit. On the other hand, when an upper type is not materialized, image I' of record data is the image which is not the image I photoed with the above-mentioned image input unit. That is, the value of D'cam (skcam, c (I)) is Dcam (the values of sk<SUB>cam and c (I) differ, or it is the case of ******** from which both image data I' and digital signature D'cam (skcam, c (I)) differ, and it can be judged that it is not image data photoed and formed with the above-mentioned image input device.).
[0058] [6th operation gestalt] With this operation gestalt, a digital camera is taken up as an example of an image input device, and the case where both a digital camera and pocket equipment have the private key of public key encryption as confidential information of a proper, respectively is explained using drawing 2 , using public key encryption as a digital signature algorithm.
[0059] Each square block shown in the block diagram 2 of a digital camera is the component of a functional order, and the line which connects them expresses a control bus and a data bus. IMG is the image pick-up section, photos the target photographic subject and changes it into an electrical signal. PRC is the image-processing section, performs suitable signal processing, A/D-conversion processing, an image processing, information source coding processing, etc. to the electric video signal formed in the above-mentioned image pick-up section IMG, and forms the digital data used as the output from a digital camera.
[0060] CPU is a central processing unit, performs predetermined count according to the control software memorized by ROM, using DRAM as a calculating field, and controls the whole camera through a bus. Above ROM is read, is the memory section of dedication and memorizes the control software required for control of a camera of a control program, a compression conversion, an indicative data, etc., etc. Above DRAM is the memory section which can be written and is used for a working-level month for CPU to calculate.
[0061] STRG is the memory section and records the photoed image data, voice data, or its part. CODEC is the digital signature generation section, has memorized the private key and the signature generation algorithm, and generates the digital signature to inputted digital one and image data using these.
[0062] It is an interface based on [based on an interface with an external device in I/F] PCMCIA specification with an external device in PCMCIA, and the image input device of this operation gestalt communicates image data, the control software, situation data, etc. with external devices, such as a

computer and memory, through these interfaces. Media Interface Connector is the voice input section, collects voice and changes it into an electrical signal. A display and LED are lamps, a control unit and LCD output and input information which a user needs using these, and OP-SW operates a camera.

[0063] In such a configuration, the basic actuation in an image input is as follows. That is, when photoing a certain object and performing an image input, pocket equipment is connected to interface I/F with the external device in a camera, and a photography person inputs directions of photography from control unit OP-SW.

[0064] CPU and pocket equipment communicate through interface I/F with an external device, and ask for the digital signature to the image photoed and formed and the data which compressed the audio digital data using the private key memorized by pocket equipment, a digital signature generation algorithm, and the private key and digital signature generation algorithm which are memorized in the camera.

[0065] The image data which carried out [above-mentioned] photography, and the recorded voice data are recorded on the memory section STRG according to the directions from an operator, or is sent to an external device through an interface with an external device, or the both are performed. In addition, a digital signature may be generated once the digital data recorded [was photoed and] and formed is recorded on the memory section STRG.

[0066] Here, it is [algorithm / in the digital camera of this operation gestalt / digital signature generation / private key / Dcan and] pkcam about Ecam and a public key in skcam and a digital signature verification algorithm. It carries out. The above-mentioned digital signature generation algorithm Dcam Private key skcam It memorizes inside the digital signature generation section CODEC. Moreover, the compression conversion algorithm h is memorized by ROM.

[0067] Moreover, it is Dman about skman and a digital signature generation algorithm in the private key stored in pocket equipment. It is Eman about pkman and a digital signature verification algorithm in the public key which corresponds by carrying out. It carries out. It is the digital signature verification algorithm Ecam of a proper to the above-mentioned digital camera. The algorithm Eman of digital signature verification of a proper to a public key pkcam and the above-mentioned pocket equipment, and a public key pkman and the compression conversion algorithm h are known by the entity (it is called a verification person) which checks the justification of data at least.

[0068] In the above digital cameras, a concrete procedure in case a digital signature is generated is as follows.

[0069] The digital signature generation CPU generates Data Dcam (skcam, h (I)) from the digital image formed with the digital camera, and voice data I, and sends it to pocket equipment through interface I/F with an external device. Pocket equipment is a private key skman. A digital signature generation algorithm and Dman It uses, count of Dman (skman and Dcan (skcam, h (I))) is performed using the sent data Dcam (skcam, h (I)), and the count result is sent to a camera through interface external I/F with an external device.

[0070] And the digital data I and digital signature Dman (skman and Dcam (skcam, h (I))) which were formed by doing in this way are recorded on the memory section STRG, it is sent to an external device through the interface PCMCIA with an external device, or the both are performed.

[0071] Moreover, a concrete procedure whose digital signature corresponding to the data and it which were photoed verifies whether it is data photoed with the above-mentioned camera when surely the above-mentioned pocket equipment is connected is as follows.

[0072] Digital signature verification record data (the verification person who received digital data I' and digital signature D'man (referred to as skman and Dcam (skcam, h (I)))) It is the digital signature verification algorithm Eman of a proper to pocket equipment. A public key pkman The digital signature verification algorithm Ecam of a proper, and a public key pkcam and the compression conversion algorithm h are used for a camera, and it is h(I') =Ecam (pkcam and Eman (pkman and D'man (skman and Dcan (skcam, h ()))))). [I]) --

It checks whether it is **********.

[0073] Here, when an upper type is materialized, record data I' is data photoed with the above-mentioned camera, when the above-mentioned pocket equipment is connected. On the other hand, when an upper type is not materialized, record data I' is data which are not the data I photoed with the above-mentioned camera, when the above-mentioned pocket equipment is connected. That is, it can be judged that the value of D'man (skman, I) is not data by which the value of Dman (skman, I) was photoed with the above-mentioned camera when it was the case of ******** from which it differs or both digital data I' and digital signature D'man (skman, I) differ and the above-mentioned pocket equipment was connected.

[0074] [other operation gestalten] -- the 1- explained above -- all the image input units and image input system which are obtained in the combination of the 6th operation gestalt are contained in the object of this invention. The conceptual diagram of the image input system which also includes the procedure of verification in addition to an image input unit is shown in drawing 3 .

[0075] drawing 3 -- setting -- image input device -- the 1- the image input unit of the 6th operation gestalt, and portable device is pocket equipment and these are connected through external I/F. Moreover, check device is the equipment for performing digital signature verification processing, and portble device2. portable device It is the same pocket equipment and connects through I/F.

[0076] For example, verification equipment check device is the digital signature verification algorithm Ecam of a proper to an image input device. It is the digital signature verification algorithm Eman of a proper to a public key pkcam and pocket equipment. Public key pkman The read personal computer or the above-mentioned digital signature verification algorithm Ecam A public key pkcam and the above-mentioned digital signature verification algorithm Eman Public key pkman It is the bar SONARU computer which connected the stored pocket equipment portable device2.

[0077] Image It is the object of photography and an image input device is the candidate Image for photography. The digital image data photoed and formed are I. In addition, pocket equipment portable device equivalent to the above-mentioned pocket equipment portable device2 The image input unit image input device connected through external I/F is able to turn into verification equipment check device.

[0078] The image data I are digital signature (if [required] and since it be compressed and curves) generation section C-CODEC. It reaches, interface external I/F with an external device is minded, and it is pocket equipment portabledevice. It is inputted at least into one side, or is digital signature generation section C-CODEC. It is outputted and inputted between interface external I/F, or the both are performed.

[0079] O The notation of + enclosed with the mark shows the processing which compounds an input, and is digital signature generation section C-CODEC. And pocket equipment portable device The final output from at least one side and the image data I are compounded and outputted. The example of the output form at this time is shown in drawing 4 . Drawing 4 is in the condition which the digital signature to the image data I and its image data I is connected, and is made into the bundle.

[0080] In addition, with the above operation gestalt, the digital signature to the image data I and its image data I was outputted. On the other hand, what is necessary is to record only a digital signature, to send to an external device, or just to perform the both, if the image data I are not compressed when using the algorithm which can restore the information on original from a digital signature like RSA cryptograph. The example in this case is shown in drawing 5 . Moreover, the example of the output form at this time is shown in drawing 6 .

[0081] In addition, the object of this invention is not restricted to the digital camera stated with the 6th operation gestalt. For example, this invention can be applied to image input units, such as a scanner, a copying machine, facsimile, a filing system, and OCR equipment, and all image input system including the verification means corresponding to them is contained in the object of this invention. moreover, information also with the target data common [not only an image but voice, text, etc.] -- application

******* -- things cannot be overemphasized.

[0082]

[Effect of the Invention] As explained above, when according to this invention what is not an operator holding the external device connected to an image input device or it cannot generate the digital signature corresponding to image data and an alteration and forgery are made to output data, it becomes possible to constitute and employ the whole system so that they may be detected using the public key of the above-mentioned equipment or the above-mentioned photography person.

[0083] Therefore, it becomes possible to guarantee that it is data with which the image data was photoed by the operator who was being generated or holds the external device with the image input unit to be sure, the certification capacity as a factual proof can be given to digital image data, and it can prevent now un-arranging [to which an application will be limited].

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the configuration of the image input device which is 1 operation gestalt of this invention.

[Drawing 2] It is the block diagram showing the configuration of the digital camera which is an example of the image input device by this operation gestalt.

[Drawing 3] It is the block diagram showing the example of a configuration of the image input system by this operation gestalt.

[Drawing 4] It is drawing showing the example of data in case an output form is composition with image data and a digital signature.

[Drawing 5] It is the block diagram showing the example of a configuration of the image input system in the case of outputting only a digital signature.

[Drawing 6] An output form is drawing showing the example of the data only in the case of a digital signature.

[Description of Notations]

imaging method Image pick-up section

memory for control program The memory section for control-software storage

work memory The memory section of the working-level month of CPU

operation switch Control unit

motor Device right hand side

memory for recorded data The memory section of image data

external I/F Interface with an external device

C-CODEC Digital signature generation section

・IMG Image pick-up section
PRC Image-processing section
CPU Central processing unit
ROM The memory section only for readouts
DRAM The memory section which can be written
STRG The memory section which records image data and voice data
CODEC Digital signature generation section
I/F Interface with an external device
PCMCIA Interface based on PCMCIA specification with an external device
Media Interface Connector Voice input section
OP-SW Control unit
LCD Display
LED Lamp

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－200730

(43)公開日　平成９年(1997)７月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｎ	7/167			Ｈ０４Ｎ	7/167		
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ａ	
			7259－5Ｊ			６４０Ｄ	
Ｈ０４Ｌ	9/32		9382－5Ｋ	Ｈ０３Ｍ	7/30	Ｚ	
Ｈ０４Ｎ	5/91			Ｈ０４Ｌ	9/00	６７５Ａ	

審査請求　未請求　請求項の数８　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平8－3603

(22)出願日　平成８年(1996)１月12日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　大石　和臣
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

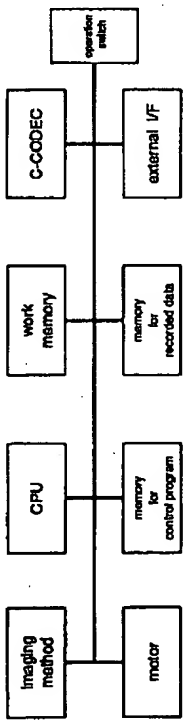
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　映像入力装置および映像入力システム

(57)【要約】

【課題】　形成されたディジタル映像データの正当性を認証することを可能にする映像入力装置を提供する。

【解決手段】　映像を入力してディジタル変換する映像入力装置において、上記映像入力装置に固有の秘密情報（例えば、公開鍵暗号系のディジタル署名方式で使用される秘密鍵）と、上記ディジタル変換された映像データとに基づき、上記映像データを識別するディジタル署名を生成するディジタル署名生成部C-CODECを設け、形成した映像データに対して、映像入力装置だけが生成できるディジタル署名を求め、映像データとそれに対応するディジタル署名とを映像入力装置の出力データとすることにより、ある映像データを形成する映像入力装置以外のものがそれに対応するディジタル署名を生成できないようにするとともに、出力データに対して改ざんや偽造がなされたときは、それを検出できるようにする。



1

【特許請求の範囲】

【請求項１】　映像を入力してディジタル・データに変換する映像入力装置において、

上記映像入力装置に固有の秘密情報および上記映像入力装置に接続される外部装置に固有の秘密情報の少なくとも一方の情報と、上記変換されたディジタル・データとに基づき、所定の演算を実行し、上記ディジタル・データを識別する情報を生成する手段を有することを特徴とする映像入力装置。

【請求項２】　上記所定の演算として、公開鍵暗号系を用いるディジタル署名方式の演算を実行することを特徴とする請求項１に記載の映像入力装置。

【請求項３】　上記所定の演算を、上記映像入力装置の内部および上記映像入力装置に接続される外部装置の内部の少なくとも一方において実行することを特徴とする請求項１または２に記載の映像入力装置。

【請求項４】　上記映像入力装置に入力され変換されたディジタル・データに対して圧縮変換を行なう手段と、

上記圧縮変換された結果のデータに対して上記所定の演算を行なうように制御する手段とを有することを特徴とする請求項１～３の何れか１項に記載の映像入力装置。

【請求項５】　映像を入力してディジタル・データに変換する映像入力システムにおいて、

上記映像入力システムに固有の秘密情報および上記映像入力システムに接続される外部装置に固有の秘密情報の少なくとも一方の情報と、上記変換されたディジタル・データとに基づき、所定の演算を実行し、上記ディジタル・データを識別する情報を生成する手段と、

上記ディジタル・データを識別する情報を用いて、上記生成されたディジタル・データが確かに上記映像入力システムで生成されたものかどうかを検証する手段とを有することを特徴とする映像入力システム。

【請求項６】　上記所定の演算として、公開鍵暗号系を用いるディジタル署名方式の演算を実行することを特徴とする請求項５に記載の映像入力システム。

【請求項７】　上記所定の演算を、上記映像入力システムの内部および上記映像入力システムに接続される外部装置の内部の少なくとも一方において実行することを特徴とする請求項５または６に記載の映像入力システム。

【請求項８】　上記映像入力システムに入力され変換されたディジタル・データに対して圧縮変換を行なう手段と、

上記圧縮変換された結果のデータに対して上記所定の演算を行なうように制御する手段とを有することを特徴とする請求項５～７の何れか１項に記載の映像入力システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、映像入力装置および映像入力システムに関する。

2

【０００２】

【従来の技術】映像を入力してディジタルの映像データを形成する映像入力装置や映像入力システムは、映像データの高精細化および高画質化と、装置あるいはシステムの低コスト化とが追求されることが一般的である。そのために、高解像度の入力デバイスや効率の良い符号化、および小型化のための技術等が広範に研究開発されている。

【０００３】これに対し、形成されたディジタルの映像データが確かにその映像入力装置あるいは映像入力システムで形成されたことを保証する技術を機能として組み込むことは、従来あまり考えられていなかった。

【０００４】

【発明が解決しようとする課題】アナログの映像入力装置では、形成される映像はアナログ・データであるため、その映像データの改ざんあるいは偽造を行うためには特殊な知識、能力等が必要であり、結果的に改ざんや偽造が成功することは少なかった。これに対して、ディジタルの映像データの場合は、比較的容易に改ざんや偽造が行なわれ得るため、映像データの信憑性が低いという問題があった。

【０００５】例えば、銀塩写真のネガ・フィルムに記憶されている映像は、銀塩分子により構成されているため、これを見破って改ざんや偽造を行うことは困難である。これに対して、ディジタル・データで表現されている映像は、０と１のビット列から構成されているため、コンピュータを用いて改ざんや偽造が行なわれやすい。したがって、ディジタルの映像データは、事実の証拠としての証明能力が小さい、すなわち信憑性が低いと言え、用途が限定される恐れがある。

【０００６】本発明はこのような問題を解決するために成されたものであり、形成されたディジタル映像データの正当性を認証することができるようにした映像入力装置および映像入力システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の映像入力装置およびシステムは、ディジタル・データの正当性を保証するための技術であるディジタル署名を応用する。ディジタル署名とは、岡本栄司著の暗号理論入門（共立出版株式会社）によれば、「メッセージや情報の作成者が確かにそれらを作成したことを示す」ものである。つまり、ユーザや、計算機等の通信または計算処理を行なう主体（エンティティと呼ぶ）があるディジタル・データを認めたときに、その事実を示す証拠として用いられるディジタル・データである。

【０００８】本発明の映像入力装置は、形成したディジタルの映像データに対して、映像入力装置だけが生成できるディジタル署名を求め、映像データ自体とそれに対応するディジタル署名とを映像入力装置の出力データと

する。そして、本発明の映像入力システムにおいて、上記出力データを受け取ったエンティティは、映像データとディジタル署名との対応関係が正しく成り立つかどうかを確認し、正しい対応関係が認められないデータは正当ではないとする。

【０００９】上述の手段により、あるディジタル映像データを形成する映像入力装置以外のものは、その映像データに対応するディジタル署名を生成することはできず、かつ、出力データに対して改ざんや偽造がなされたときは、それを検出することが可能になる。したがって、その映像データが確かにその映像入力装置で生成されたものだということを保証することが可能になり、ディジタル映像データに事実の証拠としての証明能力を与えることができる。

【００１０】

【発明の実施の形態】

〔第１の実施形態〕本実施形態では、ディジタル署名のアルゴリズムとして公開鍵暗号を用い、映像入力装置の内部に固有の秘密情報として公開鍵暗号を有する場合について説明する。ただし、これは１つの例であり、公開鍵暗号を用いるディジタル署名アルゴリズムの代わりに、元情報と秘密情報とに基づいて元情報を識別する情報を生成する手段を有するものは本実施形態に全て含まれる。

【００１１】以下では、最初に公開鍵暗号について説明する。次に、映像入力装置の構成について説明し、公開鍵暗号を用いたディジタル署名を適用した本実施形態の映像入力装置がディジタル署名を生成するときの具体的な手続きを述べる。最後に、映像入力システムの機能の一部として、そのディジタル署名を検証するときの具体的な手続きについて説明する。

【００１２】公開鍵暗号

公開鍵暗号とは、暗号鍵と復号鍵とが異なり、暗号鍵を公開するとともに復号鍵を秘密に保持する暗号方式である。公開鍵暗号は、送られてきた通信文の送信者が偽者でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現でき、ディジタル署名を実現する有力な技術だと考えられている。

【００１３】例えば、通信文Mに対して、公開の暗号鍵k_pを用いて行う暗号化操作を$E(k_p, M)$とし、秘密の復号鍵k_Sを用いて行う復号操作を$D(k_S, M)$とすると、公開鍵暗号アルゴリズムは、まず次の２つの条件を満たす。

（１）暗号鍵k_pが与えられたとき、暗号化操作$E(k_p, M)$の計算は容易である。また、復号鍵k_Sが与えられたとき、復号操作$D(k_S, M)$の計算は容易である。

（２）もしユーザが復号鍵k_Sを知らないなら、暗号鍵k_pと暗号化操作$E(k_p, M)$の計算手順とC＝$E(k_p, M)$とを知っていても、通信文Mを決定することは計算量の点で困難である。

【００１４】次に、上記（１）、（２）の条件に加えて、次の（３）の条件が成立することにより秘密通信機能が実現できる。

（３）全ての通信文（平文）Mに対し暗号化操作$E(k_p, M)$が定義でき、

$D(k_S, E(k_p, M)) = M$

が成立する。つまり、暗号鍵k_pは公開されているため誰もが暗号化操作$E(k_p, M)$の計算を行うことができるが、$D(k_S, E(k_p, M))$の計算をして通信文Mを得ることができるのは復号鍵k_Sを持っている本人だけである。

【００１５】一方、上記（１）、（２）の条件に加えて、次の（４）の条件が成立することにより認証機能が実現できる。

（４）全ての通信文（平文）Mに対し復号操作$D(k_S, M)$が定義でき、

$E(k_p, D(k_S, M)) = M$

が成立する。

【００１６】つまり、復号操作$D(k_S, M)$の計算ができるのは復号鍵k_Sを持っている本人のみであり、他の人が偽の秘密鍵k_S'を用いて$D(k_S', M)$の計算を行い、復号鍵k_Sを持っている本人になりすましたとしても、

$E(k_p, D(k_S', M)) \neq M$

なので、受信者は受けとった情報が不正なものであることを認識できる。また、$D(k_S, M)$の値が改ざんされても$E(k_p, D(k_S, M)') \neq M$となり、受信者は受けとった情報が不正なものであることを確認できる。この復号操作$D(k_S, M)$を通信文Mに対するディジタル署名と呼ぶ。

【００１７】以下に、代表的な公開鍵暗号方式を挙げる。上述の秘密通信と認証通信とを行うことができる方式として、ＲＳＡ暗号（R.L.Rivest, A.Shamir and L.Adleman: “A method of obtaining digital sinnatures and public key cryptosystems”, Comm. of ACM 1987）、R暗号（M.Rabin: “Digitalized signatures and public-key cryptosystems”, MIT/LCS/TR-212, Technical Report MIT.1979）、W暗号（H.C.Williams: “A modification of the RSA public-key encryption procedure”, IEEE Trans. Inf. Theory, IT-26, 6, 1980）、ＭＩ暗号（松本，今井：“公開鍵暗号系の新しいアルゴリズム”，信学技報，IT82-84, 1982; T.Matsumoto and H.Imai: “A class of asymmetriccryptosystems based on polynomials over finite rings”, IEEE International Symp. on Infomation Theory, 1983）などがある。

【００１８】また、秘密通信のみができる方式として、ＭＨ暗号（R.C.Merkle and M.E.Hellman: “Hidding infomation and signatures in trapdoor knapsacks”, IEEETrans. Inf. Theory, IT-24, 5, 1987）、ＧＳ信号

(A. Shamir and R. E. Zippel: "On the security of the Merkle-Hellman cryptographic schme ", IEEE Trans. Inf. Theory, IT-26, 3, 1980)、CR暗号 (B. Chor and R. L. Rivest: "A knapsack type public key cryptosysts ems based on arithmetric in finit field", Proc. Crypto84)、M暗号 (R. J. McEliece: "A public-key cryptosystem based on algebraic cording theory " DSN Progress Rwp., Jet Propulsion Lab., 1978)、E暗号 (T. E. ElGamal: "A Public key cryptosystem and a signature scheme based on discretre logarithm ", Proc. Crypto 84, 1984)、T暗号 (辻井重男、"行列分解を利用した公開鍵暗号の一方式", 信学技報, IT85-12, 1985) などがある。

【0019】さらに、認証通信のみができる方式として、S暗号 (A. Shamir: "A fast signature scheme ", Report MIT/LCS/TM-107, MIT laboratory for computer science, Cambridge, Mass., 1978)、L暗号 (K. Lieberherr: "Uniform complexity and digital signature", Lecture Notes in Computer Science 115 Automata, Language and programming, Eighth Colloquium Acre, Israel, 1981)、GMY暗号 (S. Goldwasser, S. Micali and A. Yao: "Strong signature schemes", ACM Symp. on Theory of Computing, 1983)、GMR暗号 (S. Goldwasser, S. Micali and R. L. Rivest: "A "paradoxical " solution to the signature problem ", ACM Symp. on Foundation of Computer Science, 1984)、OSS暗号 (H. Ong, C. P. Schnorr and A. Shamir.: "An efficient signature scheme based on quadratic equation ", ACM Symo. on Theory of Computing 1984)、OS暗号 (岡本、白井、: "多項式演算によるディジタル署名方式、信学論 (D)、J68-D, 5, 1985; T. Okamoto and A. Shiraisi: "A fast signature scheme based on quadratic inequaliteis ", IEEE Symp. on Theory of Computing, 1984) などがある。

【0020】映像入力装置の構成

次に、上記のような公開鍵暗号を用いたディジタル署名を適用した本実施形態の映像入力装置について、図1を用いて説明する。図1に示した四角の各ブロックは機能別の構成要素であり、それらを結ぶ線は制御バス及びデータバスを表す。imaging methodは撮像部であり、対象となる被写体を撮影して電気信号に変換し、適当な信号処理、A/D変換処理、画像処理、情報源符号化処理等を行ない、ディジタル・データを出力する。

【0021】CPUは中央演算装置であり、memory for control programに記憶されている制御ソフトウェアに従い、所定の計算および制御を行なう。上記memory for control programはメモリ部であり、上記制御ソフトフェアを記憶する。work memory はメモリ部であり、CPUが計算を行なうための作業用に使われる。operation switchは操作部であり、装置を使用するユーザが種々の

指示を入力するためのものである。

【0022】motor は機構動作部であり、CPUの制御に応じて図示しない機械的な動作機構を制御する。memory for recorded dataはメモリ部であり、本装置が出力する映像データあるいはその一部を記録する。external I/Fは、コンピュータあるいは着脱可能なメモリ等の外部装置とのインターフェイス部であり、映像データや制御ソフトウェア等を上記外部装置との間で通信する。C-CODEC はディジタル署名生成部であり、入力されたディジタル・データに対するディジタル署名を生成する。

【0023】このような構成において、映像入力における基本動作は、以下の通りである。すなわち、ある対象を撮影して映像入力を行なうとき、操作者は、操作部operation switchからその指示を入力する。CPUは、その撮影指示と、メモリ部memory for control programに記憶されている制御ソフトウェアとに従って、撮像部imaging methodや機構動作部motor を制御して対象を撮影し、その撮影により形成された映像のディジタル・データをディジタル署名生成部C-CODEC に入力する。ディジタル署名生成部C-CODEC は、入力されたディジタル・データに対応するディジタル署名を生成する。

【0024】そして、このようにして形成された映像データとそれに対応するディジタル署名は、操作者からの指示に応じて、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。なお、撮影して形成されたディジタル・データが一度メモリ部memory for recorded dataに記録された後にディジタル署名生成部C-CODEC に入力されることもあり得る。

【0025】次に、以上のような映像入力装置に対して公開鍵暗号を用いるディジタル署名を適用して、装置内に固有の秘密情報として秘密鍵を有する場合について説明する。

【0026】本実施形態による映像入力装置の秘密鍵 (復号鍵) をsk_{cam}、ディジタル署名生成アルゴリズムをD_{cam}、公開鍵 (暗号鍵) をpk_{cam}、ディジタル署名検証アルゴリズムをE_{cam}とする。秘密鍵sk_{cam}とディジタル署名生成アルゴリズムD_{cam}は、ディジタル署名生成部C-CODEC の内部に記憶されている。また、公開鍵pk_{cam}とディジタル署名検証アルゴリズムEcam は、少なくともデータの正当性を確認するエンティティ (検証者と呼ぶ) には知られている。

【0027】上記のような映像入力装置において、ディジタル署名が生成されるときの具体的な手続きは次のようになる。

【0028】ディジタル署名生成

本実施形態の映像入力装置で形成されたディジタル映像データIは、ディジタル署名生成部C-CODEC に入力される。ディジタル署名生成部C-CODEC は、その内部に記憶

7

されている秘密鍵sk_{cam}とディジタル署名生成アルゴリズムD_{cam}とを用いてD_{cam}（sk_{cam}，I）を計算し、ディジタル署名として出力する。そして、このようにして得られる映像データIとディジタル署名D cam（sk_{cam}，I）は、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００２９】また、映像データとそれに対応するディジタル署名とが確かに上記の映像入力装置によって入力された映像であるか否かを検証する具体的な手続きは、以下のようになる。なお、映像入力装置に加えて以下に述べる検証の手続きも含めたシステム全体を、映像入力システムという。

【００３０】ディジタル署名検証

映像データI′とディジタル署名D′cam（sk_{cam}，I）を受け取った検証者は、公開鍵pk_{cam}とディジタル署名検証アルゴリズムE_{cam}とを用いて、

I′＝E_{cam}（pk_{cam}，D′cam（sk_{cam}，I））

が成り立つかどうかを確認する。

【００３１】ここで、上式が成立した場合は、受け取った映像データI′は上記映像入力装置で撮影された映像データIである。一方、上式が成立しない場合は、受け取った映像データI′が上記映像入力装置で撮影された映像データIではない映像になっている。すなわち、D′cam（sk_{cam}，I）の値がD_{cam}（sk_{cam}，I）の値とは異なる、あるいは映像データI′とディジタル署名D′cam（sk_{cam}，I）との両方が異なる、のいずれかの場合であり、上記装置で撮影、形成された映像データではないと判断することができる。

【００３２】〔第２の実施形態〕本実施形態では、ディジタル署名アルゴリズムとして公開鍵暗号を用い、映像入力装置に接続される外部装置に固有の秘密情報として公開鍵暗号の秘密鍵を有する場合について、図１を用いて説明する。

【００３３】本実施形態においては、次に述べる外部装置としての携帯装置（図示せず）に収められている秘密鍵をsk_{man}、ディジタル署名生成アルゴリズムをD man とし、対応する公開鍵をpk_{man}、ディジタル署名検証アルゴリズムをE_{man}とする。また、上記携帯装置は、携帯型の情報処理装置であり、撮影の際には、外部装置とのインターフェイスexternal I/Fを介して映像入力装置に接続されるものである。映像データの正当性を確認するエンティティ（検証者と呼ぶ）は、ディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}とを知っている。

【００３４】映像入力における基本動作は、以下の通りである。すなわち、ある対象を撮影して映像入力を行なうとき、上記携帯装置は映像入力装置内の外部装置とのインターフェイスexternal I/Fに接続され、撮影者は、

8

操作部operation switchから撮影の指示を入力する。ＣＰＵは、その撮影指示と、メモリ部memory for control programに記憶されている制御ソフトウェアに従って、撮像部imaging methodや機構動作部motor を制御して対象を撮影し、それにより得られる映像のディジタル・データをディジタル署名生成部C-CODEC に入力する。

【００３５】ＣＰＵと携帯装置は、外部装置とのインターフェイスexternal I/Fを介して通信する。これにより、ディジタル署名生成部C-CODEC は、携帯装置に記憶されている秘密鍵sk_{man}とディジタル署名生成アルゴリズムD_{man}とを得て、これらの情報を用いて、上記撮影して形成された映像データに対するディジタル署名を求める。

【００３６】このようにして形成された映像データとそれに対応するディジタル署名は、操作者からの指示に応じて、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。なお、撮影して形成されたディジタル・データが一度メモリ部memory for recorded dataに記録された後にディジタル署名生成部C-CODEC に入力されることもあり得る。

【００３７】以上のような映像入力装置において、ディジタル署名が生成されるときの具体的な手続きは次のようになる。

【００３８】ディジタル署名生成

ＣＰＵは、外部装置とのインターフェイスexternal I/Fを介して携帯装置から秘密鍵sk_{man}とディジタル署名生成アルゴリズムD_{man}とを映像入力装置内のメモリ部work memory とＣＰＵとにダウンロードする。次に、映像入力装置内で形成されたディジタル映像データＩを用いてD_{man}（sk_{man}，I）を計算し、それをディジタル署名として出力する。そして、このようにして得られる映像データＩとディジタル署名D_{mam}（sk_{mam}，I）は、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００３９】また、映像データとそれに対応するディジタル署名とが確かに上記の携帯装置が接続されたときに入力された映像であるか否かを検証する具体的な手続きは、以下のようになる。

【００４０】ディジタル署名検証

記録データ（映像データI′とディジタル署名D′man（sk_{man}，I）とする）を受け取った検証者は、ディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}とを用いて、

I′＝E_{man}（pk_{man}，D′man（sk_{man}，I））

が成り立つかどうかを確認する。

【００４１】ここで、上式が成立した場合は、記録デー

タの映像Ｉ′は上記携帯装置が接続されたときに撮影された映像Ｉである。一方、上式が成立しない場合は、記録データの映像Ｉ′が上記携帯装置が接続されたときに撮影された映像Ｉではない映像になっている。すなわち、D'_{man}（sk_{man}，Ｉ）の値がD_{man}（sk_{man}，Ｉ）の値とは異なる、あるいは映像データＩ′とディジタル署名D'_{man}（sk_{man}，Ｉ）との両方が異なる、のいずれかの場合であり、上記携帯装置が接続されたときに撮影された映像データではないと判断することができる。

【００４２】したがって、このような映像入力システムにおいて、携帯装置が撮影者と正確に一対一に対応していれば、撮影者が撮影した映像であることを保証するシステムが実現できる。

【００４３】〔第３の実施形態〕本実施形態では、ディジタル署名アルゴリズムとして公開鍵暗号を用い、映像入力装置に接続される外部装置に固有の秘密情報として公開鍵暗号の秘密鍵を有するとともに、その携帯装置が演算能力を持ち、ディジタル署名生成の手続きを以下のように行う場合について、図１を用いて説明する。

【００４４】ディジタル署名生成

ＣＰＵは、映像入力装置内で形成されたディジタル映像データＩを、外部装置とのインターフェイスexternal I/Fを介して携帯装置に送る。携帯装置は、その内部に記憶されている秘密鍵sk_{man}とディジタル署名生成アルゴリズムD_{man}とを用いて、送られて来た映像データＩからディジタル署名D_{man}（sk_{man}，Ｉ）を計算し、それを外部装置とのインターフェイスexternal I/Fを介して映像入力装置に送る。

【００４５】そして、このようにして得られた映像データＩとディジタル署名D_{man}（sk_{man}，Ｉ）は、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００４６】ディジタル署名検証

第２の実施形態と同じであるので、説明を省略する。

【００４７】〔第４の実施形態〕本実施形態では、ディジタル署名アルゴリズムとして公開鍵暗号を用い、映像入力装置とその外部装置である携帯装置との両方がそれぞれ固有の秘密情報として公開鍵暗号の秘密鍵を有する場合について、図１を用いて説明する。なお、本実施形態の処理は、以下のディジタル署名生成と検証の処理を除いて、第１の実施形態および第２の実施形態と同じである。

【００４８】ディジタル署名生成

ＣＰＵは、外部装置とのインターフェイスexternal I/Fを介して携帯装置から秘密鍵sk_{man}とディジタル署名生成アルゴリズムD_{man}とを映像入力装置内のメモリ部work memoryとＣＰＵとにダウンロードする。次に、上記映像入力装置内で形成されたディジタル映像データＩからD_{man}（sk_{man}，Ｉ）を計算し、その計算結果をディジタル署名生成部C-CODECに入力する。

【００４９】ディジタル署名生成部C-CODECは、入力されたデータD_{man}（sk_{man}，Ｉ）に対し、D_{cam}（sk_{cam}，D_{man}（sk_{man}，Ｉ））の計算を実行し、その計算結果をディジタル署名として出力する。このようにして形成された映像データＩとディジタル署名D_{cam}（sk_{cam}，D_{man}（sk_{man}，Ｉ））とは、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００５０】また、映像データとそれに対応するディジタル署名とが確かに上記携帯装置が接続されたときに上記映像入力装置で入力された映像であるか否かを検証する具体的な手続きは、以下のようになる。

【００５１】ディジタル署名検証

記録データ（映像データＩ′とディジタル署名D'_{cam}（sk_{cam}，D_{man}（sk_{man}，Ｉ））とする）を受け取った検証者は、映像入力装置に固有のディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}、および携帯装置に固有のディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}を用いて、

$I' = E_{man}(pk_{man}, E_{cam}(pk_{cam}, D'_{cam}(sk_{cam}, D_{man}(sk_{man}, I))))$

が成り立つかどうかを確認する。

【００５２】ここで、上式が成立した場合は、記録データの映像Ｉ′は上記映像入力装置で上記携帯装置が接続されたときに撮影された映像であるが、上式が成立しない場合はそれとは異なる映像であると判断することができる。

【００５３】なお、上記の実施形態では、ディジタル署名生成の順序は、最初に携帯装置で次に映像入力装置の順であったが、逆にすることも可能であり、その場合は検証の順序も逆になる。また、映像入力装置と携帯装置との両方が署名したデータをその順序にかかわりなく生成、検証することも可能である。さらに、携帯装置のディジタル署名生成アルゴリズムD_{man}を映像入力装置の内部に記憶しておき、秘密鍵sk_{man}のみを携帯装置に記憶しておくこともできる。

【００５４】〔第５の実施形態〕次に、圧縮技術を用いて、記録する映像データの代わりにそれを圧縮したデータに対してディジタル署名を生成する場合について説明する。ここでは、圧縮変換をｃで表すこととする。映像データの正当性を確認するエンティティ（検証者と呼ぶ）は、この圧縮変換ｃを知っている。その他は、上記第１～第４の実施形態と同様である。

【００５５】ディジタル署名生成

ＣＰＵは、映像入力装置内の撮像部imaging methodで形成されたディジタル映像データＩに対しｃ（Ｉ）の計算を実行し、それにより得られる圧縮データｃ（Ｉ）を映

像データＩの代わりに用いる。他の処理は、上記第１～第４の実施形態と同様である。例えば、第１の実施形態の場合に即して説明すると、映像データＩとディジタル署名D_{cam}（sk_{cam}，c（Ｉ））とがメモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００５６】ディジタル署名検証

記録データ（映像データＩ′とディジタル署名D'_{cam}（sk_{cam}，c（Ｉ）とする）を受け取った検証者は、ディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}とを用いて、

$c(I') = E_{cam}(pk_{cam}, D'_{cam}(sk_{cam}, c(I)))$

が成り立つかどうかを確認する。なお、検証者が圧縮変換の逆変換c^{-1}を知っているならば、

$I' = c^{-1}(E_{cam}(pk_{cam}, D'_{cam}(sk_{cam}, c(I))))$

が成り立つかどうかをを確認してもよい。

【００５７】ここで、上式が成立した場合は、記録データの映像Ｉ′は上記映像入力装置で撮影された映像である。一方、上式が成立しない場合は、記録データの映像Ｉ′が上記映像入力装置で撮影された映像Ｉではない映像になっている。すなわち、D'_{cam}（sk_{cam}，c（Ｉ））の値がD_{cam}（sk_{cam}，c（Ｉ）の値とは異なる、あるいは映像データＩ′とディジタル署名D'_{cam}（sk_{cam}，c（Ｉ））との両方が異なる、のいずれかの場合であり、上記映像入力装置で撮影、形成された映像データではないと判断することができる。

【００５８】〔第６の実施形態〕本実施形態では、映像入力装置の一例としてディジタル・カメラを取り上げ、ディジタル署名アルゴリズムとして公開鍵暗号を用い、ディジタル・カメラと携帯装置との両方がそれぞれ固有の秘密情報として公開鍵暗号の秘密鍵を有する場合について、図２を用いて説明する。

【００５９】ディジタル・カメラの構成

図２に示した四角の各ブロックは機能別の構成要素であり、それらを結ぶ線は制御バス及びデータバスを表す。ＩＭＧは撮像部であり、対象となる被写体を撮影して電気信号に変換する。ＰＲＣは画像処理部であり、上記撮像部ＩＭＧで形成された電気映像信号に対して適当な信号処理、Ａ／Ｄ変換処理、画像処理、情報源符号化処理等を行ない、ディジタル・カメラからの出力となるディジタル・データを形成する。

【００６０】ＣＰＵは中央演算装置であり、ＲＯＭに記憶されている制御ソフトウェアに従い、ＤＲＡＭを計算用の領域として利用しながら所定の計算を行ない、バスを介してカメラ全体の制御を行なう。上記ＲＯＭは読みだし専用のメモリ部であり、制御プログラムや圧縮変換、表示データなどの、カメラの制御に必要な制御ソフトウェアを記憶する。上記ＤＲＡＭは読み書き可能なメモリ部であり、ＣＰＵが計算を行なうための作業用に使われる。

【００６１】ＳＴＲＧはメモリ部であり、撮影した映像データや音声データあるいはその一部を記録する。ＣＯＤＥＣはディジタル署名生成部であり、秘密鍵と署名生成アルゴリズムとを記憶しており、これらを用いて、入力されたディジタル・映像データに対するディジタル署名を生成する。

【００６２】Ｉ／Ｆは外部装置とのインターフェイス、ＰＣＭＣＩＡは外部装置とのＰＣＭＣＩＡ規格に基づくインターフェイスであり、本実施形態の映像入力装置は、これらのインタフェースを介して映像データ、制御ソフトウェア、状況データ等をコンピュータやメモリ等の外部装置と通信する。ＭＩＣは音声入力部であり、音声を収集し電気信号に変換する。ＯＰ－ＳＷは操作部、ＬＣＤはディスプレイ、ＬＥＤはランプであり、これらを用いてユーザは必要な情報の入出力を行い、カメラを操作する。

【００６３】このような構成において、映像入力における基本動作は、以下の通りである。すなわち、ある対象を撮影して映像入力を行なうとき、携帯装置はカメラ内の外部装置とのインターフェイスＩ／Ｆに接続され、撮影者は、操作部ＯＰ－ＳＷから撮影の指示を入力する。

【００６４】ＣＰＵと携帯装置は、外部装置とのインターフェイスＩ／Ｆを介して通信し、携帯装置に記憶されている秘密鍵とディジタル署名生成アルゴリズム、およびカメラ内に記憶されている秘密鍵とディジタル署名生成アルゴリズムを用いて、撮影して形成された映像、音声のディジタル・データを圧縮したデータに対するディジタル署名を求める。

【００６５】上記撮影した映像データと録音した音声データとは、操作者からの指示に応じてメモリ部ＳＴＲＧに記録されるか、外部装置とのインターフェイスを介して外部装置に送られるか、あるいはその両方が行なわれる。なお、撮影、録音して形成されたディジタル・データが一度メモリ部ＳＴＲＧに記録された後にディジタル署名が生成されることもあり得る。

【００６６】ここで、本実施形態のディジタル・カメラにおけるディジタル署名生成アルゴリズムをD_{can}、秘密鍵をsk_{cam}、ディジタル署名検証アルゴリズムをＥcam、公開鍵をpk_{cam}とする。上記ディジタル署名生成アルゴリズムD_{cam}と秘密鍵sk_{cam}は、ディジタル署名生成部ＣＯＤＥＣの内部に記憶されている。また、圧縮変換アルゴリズムｈはＲＯＭに記憶されている。

【００６７】また、携帯装置に収められている秘密鍵をsk_{man}、ディジタル署名生成アルゴリズムをD_{man}とし、対応する公開鍵をpk_{man}、ディジタル署名検証アルゴリズムをE_{man}とする。上記ディジタル・カメラに固有のディジタル署名検証アルゴリズムE_{cam}と公開鍵

pk_{cam}、上記携帯装置に固有のディジタル署名検証のアルゴリズムE_{man}と公開鍵pk_{man}、および圧縮変換アルゴリズムhは、少なくともデータの正当性を確認するエンティティ（検証者と呼ぶ）には知られている。

【００６８】上記のようなディジタル・カメラにおいて、ディジタル署名が生成されるときの具体的な手続きは次のようになる。

【００６９】ディジタル署名生成

ＣＰＵは、ディジタル・カメラで形成されたディジタル映像及び音声データＩからデータD_{cam}（sk_{cam}，h（Ｉ））を生成し、それを外部装置とのインターフェイスＩ／Ｆを介して携帯装置に送る。携帯装置は、秘密鍵sk_{man}とディジタル署名生成アルゴリズムとD_{man}を用いて、送られて来たデータD_{cam}（sk_{cam}，h（Ｉ））を用いてD_{man}（sk_{man}，D_{can}（sk_{cam}，h（Ｉ））の計算を実行し、その計算結果を、外部装置とのインターフェイスexternal I/Fを介してカメラに送る。

【００７０】そして、このようにして形成されたディジタル・データＩとディジタル署名D_{man}（sk_{man}，D_{cam}（sk_{cam}，h（Ｉ））は、メモリ部ＳＴＲＧに記録されるか、外部装置とのインターフェイスＰＣＭＣＩＡを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００７１】また、撮影されたデータとそれに対応するディジタル署名とが確かに上記携帯装置が接続されたときに上記カメラで撮影されたデータであるか否かを検証する具体的な手続きは、以下のようになる。

【００７２】ディジタル署名検証

記録データ（ディジタル・データＩ′とディジタル署名D'_{man}（sk_{man}，D_{cam}（sk_{cam}，h（Ｉ））とする）を受け取った検証者は、携帯装置に固有のディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}、カメラに固有のディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}、および圧縮変換アルゴリズムhを用いて、

$h(I') = E_{cam}(pk_{cam}, E_{man}(pk_{man}, D'_{man}(sk_{man}, D_{can}(sk_{cam}, h(I)))))$

が成り立つかどうかを確認する。

【００７３】ここで、上式が成立した場合は、記録データＩ′は上記携帯装置が接続されたときに上記カメラで撮影されたデータである。一方、上式が成立しない場合は、記録データＩ′が上記携帯装置が接続されたときに上記カメラで撮影されたデータＩではないデータになっている。すなわち、D'_{man}（sk_{man}，Ｉ）の値がD_{man}（sk_{man}，Ｉ）の値とは異なる、あるいはディジタル・データＩ′とディジタル署名D'_{man}（sk_{man}，Ｉ）との両方が異なる、のいずれかの場合であり、上記携帯装置が接続されたときに上記カメラで撮影されたデータではないと判断することができる。

【００７４】〔その他の実施形態〕以上に説明した第１～第６の実施形態の組合せで得られる全ての映像入力装置および映像入力システムは、本発明の対象に含まれる。映像入力装置に加えて検証の手続きも含めた映像入力システムの概念図を、図３に示す。

【００７５】図３において、image input deviceは第１～第６の実施形態の映像入力装置、portable deviceは携帯装置であり、これらはexternal I/Fを介して接続されている。また、check deviceはディジタル署名検証処理を実行するための装置、portble device2 はportable device と同様の携帯装置であり、Ｉ／Ｆを介して接続される。

【００７６】例えば、検証装置check deviceは、映像入力装置に固有のディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}、および携帯装置に固有のディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}を読み込んだパーソナル・コンピュータ、あるいは、上記ディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}、および上記ディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}を格納した携帯装置portable device2を接続したパーソナル・コンピュータである。

【００７７】Image は撮影の対象であり、映像入力装置が撮影対象Image を撮影して形成したディジタル映像データがＩである。なお、上記携帯装置portable device2と同等の携帯装置portable device をexternal I/Fを介して接続した映像入力装置image input deviceが検証装置check deviceとなることも可能である。

【００７８】映像データＩは（必要ならば圧縮され、それから）ディジタル署名生成部C-CODEC および外部装置とのインタフェースexternal I/Fを介して携帯装置portabledevice の少なくとも一方に入力されるか、ディジタル署名生成部C-CODEC とインタフェースexternal I/Fとの間で入出力されるか、あるいはその両方が行われる。

【００７９】○印で囲んだ＋の記号は、入力を合成する処理を示し、ディジタル署名生成部C-CODEC および携帯装置portable device の少なくとも一方からの最終出力と、映像データＩとを合成して出力する。このときの出力形式の例を、図４に示す。図４は、映像データＩとその映像データＩに対するディジタル署名とが連結されてひとまとまりにされている状態である。

【００８０】なお、以上の実施形態では、映像データＩとその映像データＩに対するディジタル署名とが出力された。これに対し、ＲＳＡ暗号のようにディジタル署名から元の情報を復元できるアルゴリズムを用いる場合は、映像データＩが圧縮されていないならばディジタル署名のみを記録するか、外部装置に送るか、あるいはその両方を行えばよい。この場合の例を、図５に示す。また、このときの出力形式の例を図６に示す。

【００８１】なお、本発明の対象は、第６の実施形態で述べたディジタル・カメラに限られない。例えば、スキャナ、複写機、ファクシミリ、ファイリング・システム、ＯＣＲ装置等の映像入力装置に本発明を適用可能であり、それらに対応する検証手段を含めた映像入力システムは、全て本発明の対象に含まれる。また、対象とするデータも映像に限らず、音声、文字情報等の一般的な情報に適用できることは言うまでもない。

【００８２】

【発明の効果】以上説明したように、本発明によれば、映像入力装置あるいはそれに接続される外部装置を保持している操作者でないものは映像データに対応するディジタル署名を生成することができず、かつ、出力データに対して改ざんや偽造がなされたときは、上記装置あるいは上記撮影者の公開鍵を用いてそれらを検出するようにシステム全体を構成、運用することが可能になる。

【００８３】したがって、その映像データが確かにその映像入力装置で生成された、あるいはその外部装置を保持している操作者によって撮影されたデータだということを保証することが可能になり、ディジタル映像データに事実の証拠としての証明能力を与えることができ、用途が限定されてしまう不都合を防ぐことができるようになる。

【図面の簡単な説明】

【図１】本発明の一実施形態である映像入力装置の構成を示すブロック図である。

【図２】本実施形態による映像入力装置の一例であるディジタル・カメラの構成を示すブロック図である。

【図３】本実施形態による映像入力システムの構成例を示すブロック図である。

【図４】出力形式が映像データとディジタル署名との合成である場合のデータの例を示す図である。

【図５】ディジタル署名のみを出力する場合の映像入力システムの構成例を示すブロック図である。

【図６】出力形式がディジタル署名のみの場合のデータの例を示す図である。

【符号の説明】

imaging method　撮像部

memory for control program　制御ソフトウェア記憶用のメモリ部

work memory　ＣＰＵの作業用のメモリ部

operation switch　操作部

motor　機構動作部

memory for recorded data　映像データのメモリ部

external I/F　外部装置とのインターフェイス

C-CODEC　ディジタル署名生成部

ＩＭＧ　撮像部

ＰＲＣ　画像処理部

ＣＰＵ　中央演算装置

ＲＯＭ　読みだし専用のメモリ部

ＤＲＡＭ　読み書き可能なメモリ部

ＳＴＲＧ　映像データや音声データを記録するメモリ部

ＣＯＤＥＣ　ディジタル署名生成部

Ｉ／Ｆ　外部装置とのインターフェイス

ＰＣＭＣＩＡ　外部装置とのＰＣＭＣＩＡ規格に基づくインターフェイス

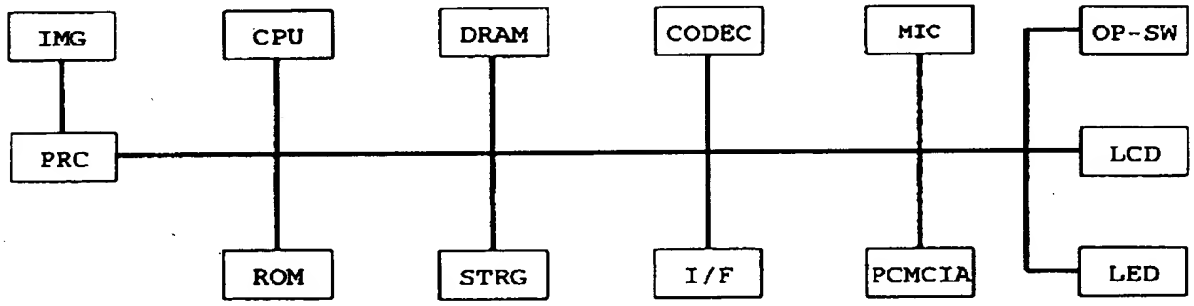
ＭＩＣ　音声入力部

ＯＰ－ＳＷ　操作部

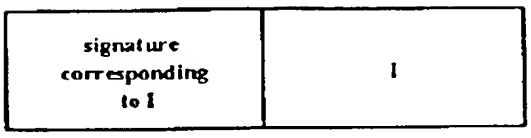
ＬＣＤ　ディスプレイ

ＬＥＤ　ランプ

【図２】

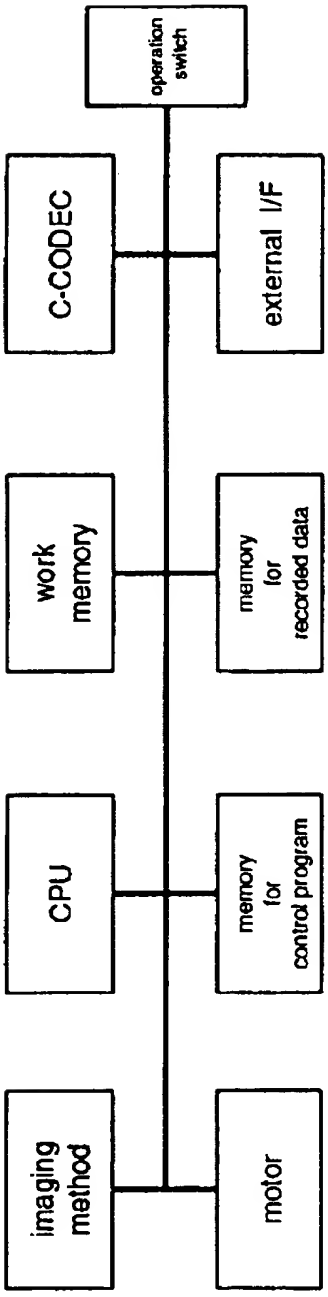


【図４】



【図６】

【図１】


operation switch
C-CODEC
external I/F
work memory
memory for recorded data
CPU
memory for control program
imaging method
motor

【図3】

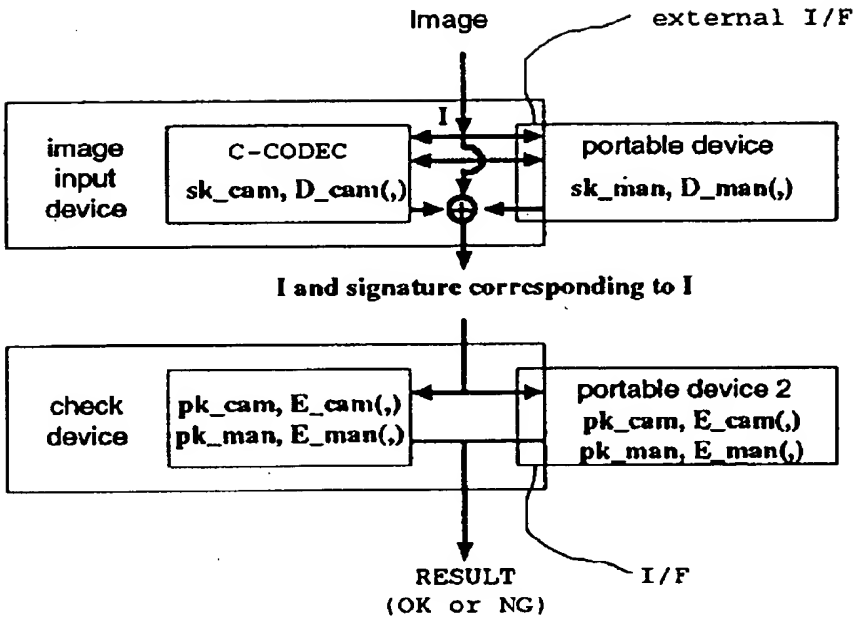


Image
external I/F
I
image input device
C-CODEC
sk_cam, D_cam(,)
portable device
sk_man, D_man(,)
I and signature corresponding to I
check device
pk_cam, E_cam(,)
pk_man, E_man(,)
portable device 2
pk_cam, E_cam(,)
pk_man, E_man(,)
RESULT
(OK or NG)
I/F

【図5】

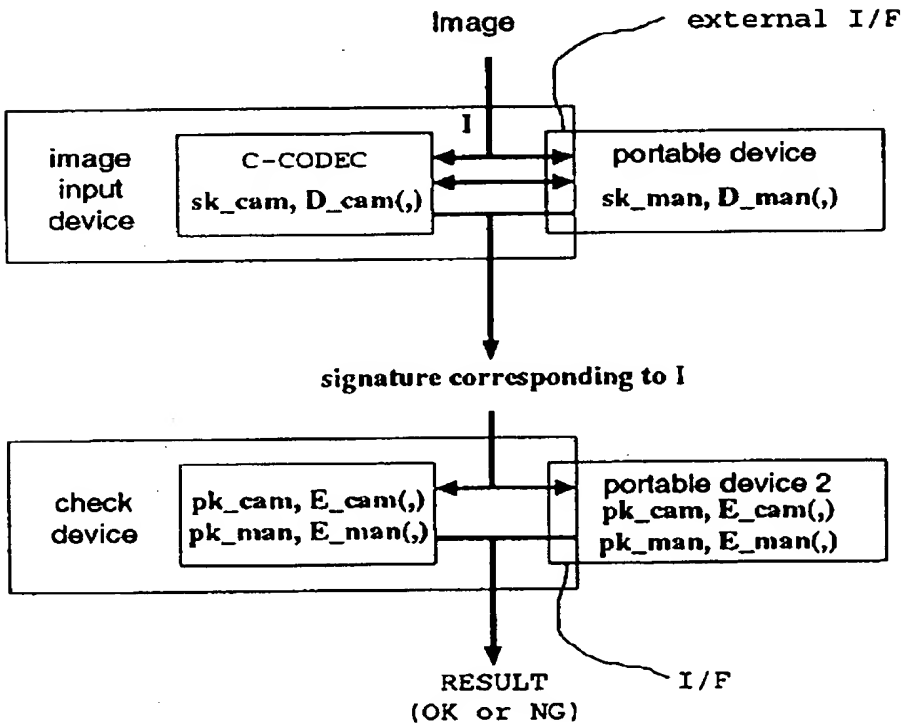


Image
external I/F
I
image input device
C-CODEC
sk_cam, D_cam(,)
portable device
sk_man, D_man(,)
signature corresponding to I
check device
pk_cam, E_cam(,)
pk_man, E_man(,)
portable device 2
pk_cam, E_cam(,)
pk_man, E_man(,)
RESULT
(OK or NG)
I/F

フロントページの続き

(51) Int. Cl. 6	識別記号	庁内整理番号	F I		技術表示箇所
// H03M 7/30			H04N 5/91	P	